3M

УДК 004.04

В.Е. Мухин
Национальный технический университет Украины
«Киевский политехнический институт», г. Киев
mukhin@comsys.ntu-kpi.kiev.ua

Средства защиты GRID-систем на основе дифференцирования уровня доверия к узлам системы

В статье предлагаются средства защиты Grid-систем на основе репутационного метода установления доверительных отношений между узлами и ранжирования информации по ее ценности. Проведенные экспериментальные исследования показали, что предложенные средства позволяют повысить уровень защищенности Grid-системы при ее масштабировании с добавлением новых узлов, что повышает эффективность системы обеспечения безопасности Grid.

Введение

В последние годы мировое научное сообщество испытывает все большую необходимость в больших вычислительных мощностях, что связано с необходимостью проведения сложных и ресурсоемких вычислений, при этом мощные вычислительные системы являются весьма дорогостоящими. В связи с этим стремительно развиваются Grid-системы, которые объединяют существующие вычислительные центры, могут просто и быстро масштабироваться и выполняют распределенные приложения, используя все доступные им ресурсы.

На данный момент существует довольно большое количество решений по организации Grid-систем. Поскольку большинство транзакций в Grid-системах происходит через открытые коммуникационные среды, возникает ряд проблем, связанных с обеспечением безопасности Grid [1]. Традиционные меры, в первую очередь, предусматривают изоляцию систем и защиту ресурсов за счет поддержки правил, ограничивающих действия пользователей, что противоречит главной идее Grid – совместному использованию ресурсов вне зависимости от географических рубежей и границ организаций [2].

Современные подходы к организации механизмов защиты информации в компьютерных системах предусматривают централизацию средств защиты (сертификационные агентства, службы регистрации и авторизации, единые для всей системы), что накладывает значительные ограничения при динамическом масштабировании систем Grid-систем [3]. Таким образом, весьма актуальной в настоящее время является проблема разработки средств обеспечения безопасности ресурсов Grid-систем.

Требования к системе безопасности GRID

Ввиду проблем, возникающих при обеспечении безопасности Grid-систем, средства безопасности Grid должны поддерживать следующие механизмы защиты [2]:

1. *Аутентификацию* – предоставление способа подключения различных механизмов аутентификации и метода их использования в различных ситуациях.

2. *Передачу прав* – предоставление средств, позволяющих осуществлять передачу прав доступа от запрашивающей стороны к вызываемой службе.

3. *Единоразовый вход* – освобождение субъектов, которые выполнили процедуру аутентификации, от необходимости ее повторения при каждой попытке доступа к ресурсам на некоторое время.

4. *Жизненный цикл мандатов и его обновление* – во многих случаях возможна ситуация, когда процесс, инициированный субъектом, выполняется дольше, чем время действия выданного мандата. Поэтому необходимо предупреждать об этом субъекта либо предусмотреть обновление мандата, для того чтобы работа могла быть закончена.

5. *Авторизацию* – разрешение доступа к службам на основании политик авторизации, связанных с ними (кто и на каких основаниях может осуществлять доступ), и предоставление возможности вызывающей стороне задавать политики выполнения (кому клиент доверяет выполнение).

6. *Конфиденциальность* – защита конфиденциальности механизма передачи данных.

7. *Целостность данных* – обеспечение обнаружения несанкционированных изменений в сообщениях с принимающей стороны.

8. *Обмен политиками* – предоставление возможности обмена информацией о политиках безопасности вызывающей и вызываемой сторонам для создания безопасной среды обмена информацией.

9. *Уровень обеспечения безопасности* – реализация средств, позволяющих определить требуемый уровень обеспечения безопасности системы.

10. *Проницаемость сетевых экранов (firewalls)* – основным барьером при передаче данных в динамических, кроссдоменных Grid - систем являются межсетевые экраны, поэтому при проектировании системы необходимо обеспечить возможность свободной передачи данных экран без изменения их политик безопасности.

Большинство из вышеперечисленных требований вошли в стандарт под названием OGSA (Security Architecture for Open Grid Services), разработанный Open Grid Forum (OGF), и на сегодняшний день Globus Toolkit (GT) – широко распространенная реализация этого стандарта.

Метод установления доверительных отношений между узлами Grid-системы

Установление доверия между узлами

Для эффективного обеспечения безопасности Grid-систем предлагается новый подход к реализации средств защиты ресурсов Grid с учетом уровня доверия к узлам и ранжирования информации по ее ценности. Суть предлагаемого подхода заключается в следующем.

Grid-система представляет собой множество узлов и объединяющих их сетей. Изначально каждый новый узел либо сеть, подключаемые к системе имеют нулевой, уровень доверия со стороны других узлов Grid, так как отсутствует предыдущий опыта использования данного узла. Вопрос установления доверия или доверительных отношений в данном случае должен рассматриваться с двух различных позиций:

– с позиции узлов, уже интегрированных в Grid-систему;
– с позиции нового узла.

С точки зрения обеспечения безопасности Grid вновь подключенному узлу нельзя предоставлять конфиденциальную информацию (с определенной степенью секретности). Единственной информацией, которую можно передавать узлу, являются лишь

открытые данные. Также необходимо четко отслеживать информацию, получаемую от нового узла, так как под видом запрашиваемых данных он может, например, передать вирус и, таким образом, причинить ущерб работе системы или осуществить несанкционированный доступ к секретным данным [4]. Узел, который подключается к Grid, автоматически принимает политику безопасности, установленную в Grid-системе, и, таким образом, доверяет как минимум узлу или сети, которая ответственна за организацию работы ядра системы.

Таким образом, очень важной проблемой является установление показателей доверия к узлам Grid-системы – репутации узла в системе на основе предыдущего опыта работы системы с узлом. Определить уровень доверия можно следующими двумя способами:

– непосредственно по опыту работы с узлом в Grid-системе;
– по данным от узлов, ранее интергрированных в Grid-систему.

Определение уровня доверия к узлу по данным от уже интегрированных узлов является достаточно простым способом. Однако ввиду того, что Grid-система объединяет достаточно большое количество узлов, получение информации от каждого из них является весьма трудоемкой задачей и требует значительного времени. Так в системе XenoTrust данная задача решается путем ограничения количества узлов, от которых принимается информация. Но в этом случае требуются четкие критерии того, от каких именно узлов брать данные и как их оценивать, поскольку в случае если репутация узла в системе не высока, то и данные предоставляемые им о доверии, тоже могут быть недостоверными или искаженными [5].

В связи с этим предлагается ввести сервер-хранилище метрик доверия. Данный сервер принимает информацию от различных узлов, и, в зависимости от уровня доверия к ним, интерпретирует полученную информацию, формируя таким образом усредненные показатели доверия (1):

$$T_{s_i} = \frac{T_{s_i} + \sum_{j=1}^{n} T_{ji} * T_{s_j}}{n+1}, \quad (1)$$

где Ts_i – показатель доверия к i-ому узлу, хранящийся на сервере метрик доверия, T_{ji} – показатель доверия j-го узла к i-ому.

Оценка уровня доверия непосредственно по опыту работы с узлом является более трудоемкой задачей, чем предыдущий способ, однако этот подход позволяет получить более достоверные результаты. В действительности сформировать уровень доверия по одной сессии невозможно, поскольку такая оценка не будет объективной, т.к. существует большая вероятность того, что злоумышленник на удаленном узле проявит себя лишь в m-той сессии. В связи с этим необходимо формировать вектор репутации узлов W_i, отображающий опыт взаимодействия Grid-системы с i-м узлом. Каждый элемент данного вектора соответствует отдельной сессии, а значение – уровню угрозы со стороны удаленного узла, при этом уровни угроз определяются на основе экспертных оценок. Уровнем угрозы, в данном случае, является вероятность выхода из строя или нестабильности работы системы узла Grid-системы из-за несанкционированных действий со стороны узлов. Если сессия прошла без несанкционированных действий, то ей присваивается значение 0. Показатель доверия рассчитывается как (2):

$$T_j = \frac{\sum_{j=1}^{n} \left(1 - W_i\right)}{n_j}, \quad (2)$$

где n_j – количество транзакций с j-ым узлом, W_i – i-е значение вектора репутации узла.

Таким образом, показатель доверия находится в интервале от 0 до 1, причем 0 соответствует полному отсутствию доверия, а 1 – полному доверию узлу со стороны Grid-системы.

Для дополнительной проверки вновь добавленного узла с начальным нулевым уровнем доверия можно использовать т.н. тестовую информацию, т.е. сгенерировать дезинформацию и передать ее узлу для оценки его реакции на нее. Необходимость в таких проверочных данных является особенно актуальной в тех случаях, когда в системе задания работают лишь с конфиденциальной информацией, которые требуют их выполнения только на доверенных узлах, степенью доверия к которым достаточна для решения на них данных заданий.

Ранжирование информации

Поскольку Grid-система включает в себя узлы с различной степенью доверия, то необходимо автоматически определять может ли определенная информация быть предоставлена удаленному узлу, для чего требуется ранжирование информации по ее ценности в Grid-системе. Рангом в данном случае выступает минимально допустимый показатель доверия к системе. Таким образом, перед передачей информации узлу ее ранг (ценность) сравнивается с показателем доверия к данному узлу, и если ранг информации меньше, чем текущий уровень доверия, то такая передача разрешена.

Ценность информации, т.е. реальная стоимость или величина убытков в случае ее уничтожения или утери конфиденциальности, изменяется в зависимости от вида информации с течением времени. В настоящее время применяется следующая классификация информации в зависимости от динамики изменения ее ценности во времени: ценность информации стационарна во времени; постоянно увеличивается; постоянно уменьшается; имеет верхний экстремум; имеет нижний экстремум [6].

Репутационный метод установления доверия к узлам

Таким образом, сформулируем предлагаемый репутационный метод установления доверия к узлам Grid-систем.

1. Выполняется ранжирование по ценности информации, которая используется при вычислениях, т.е. передается удаленным узлам. Каждый отдельный блок информации (данные, задачи и т.п.) должен иметь определенный ранг.

2. Перед каждой транзакцией с удаленным узлом выполняется проверка допустимость передачи информации данному узлу путем сравнения текущего уровня доверия к этому узлу и ранга информационного блока. Если уровень доверия к узлу больше, чем ранг (ценность) данных или заданий, то такая транзакция разрешена.

3. По окончанию каждой сессии выполняется модификация вектор репутации W_i узлов Grid-систем, при этом:

a) если были обнаружены какие-либо несанкционированные действия со стороны удаленного узла, то этот факт должен быть отражен в векторе репутации;

b) если несанкционированные действия со стороны узла не выявлены, то производится перерасчет значения уровня доверия к данному узлу.

4. В результате, после каждой сессии в Grid-системе узел получает обновленный текущий уровень доверия к нему, который используется в дальнейших сессиях.

Средства установления доверительных отношений между узлами Grid

В соответствии с рекомендациями OGF, средства обеспечения безопасности Grid-систем должны надстраиваться над уже существующими аппаратно-программными механизмами поддержки распределенных вычислений [7].

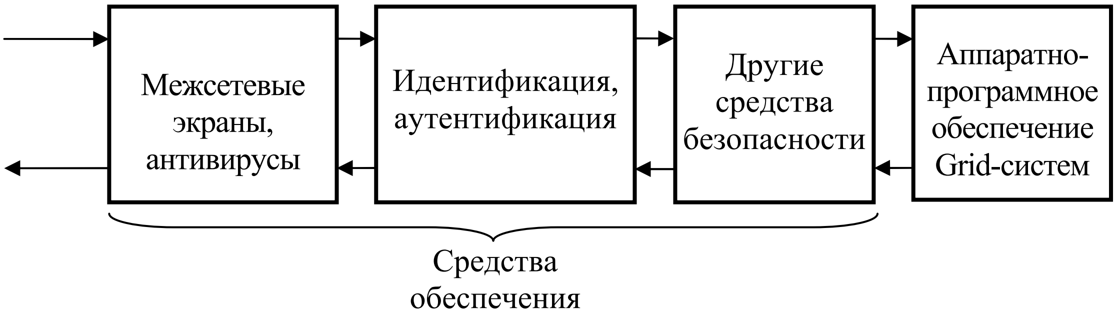


Рисунок 1 – Обобщенная схема средств обеспечения безопасности и их взаимодействие со средствами, обеспечивающими функционирование Grid

На рис. 1 приведена обобщенная схема расположения средств обеспечения безопасности. Такая кольцевая структура позволяет выделить средства обеспечения безопасности в отдельный комплекс, а не распределять их по всей системе. Данный комплекс берет на себя все функции, связанные с обеспечением безопасности.

В целом, система безопасности Grid состоит из следующих компонентов (рис. 2):
– средства обеспечения безопасности передающей среды;
– средства публикации и обмена политиками безопасности;
– средства трансляции сущностей и мандатов для разнородных систем (каковыми в большинстве являются Grid);
– средства авторизации и аутентификации;
– средства поддержки политик безопасности;
– средства управления доверием;

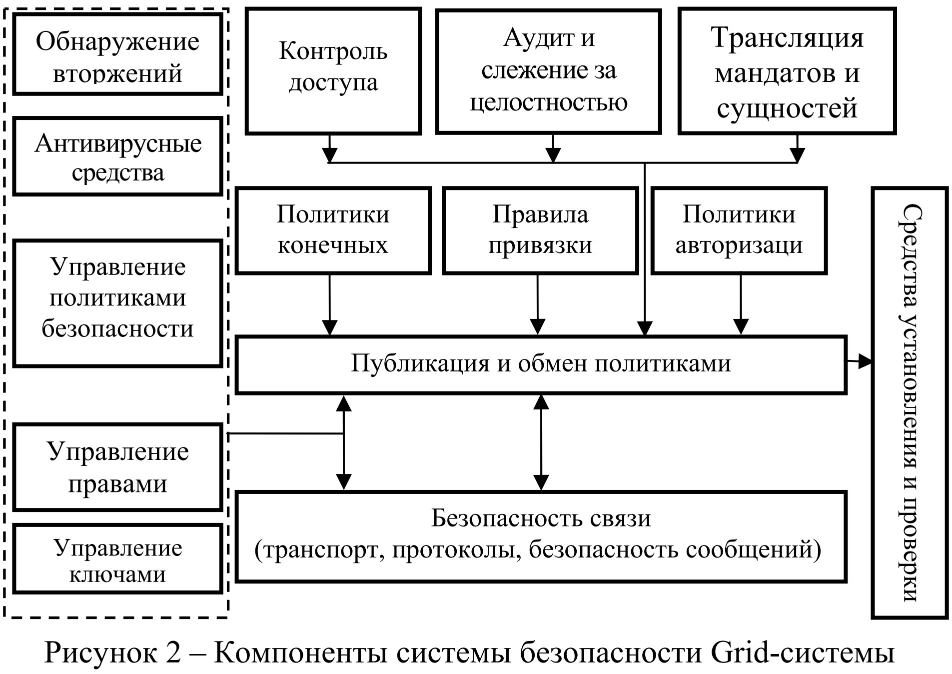


Рисунок 2 – Компоненты системы безопасности Grid-системы

– средства аудита;
– средства обнаружения вторжений;
– антивирусные средства.

Средства обеспечения безопасности связи поддерживают безопасные механизмы передачи сообщений на уровне протоколов и связей. Так, для обеспечения безопасности http-сообщений применяются протоколы SSL, TLS либо IPSec.

Последние требования и рекомендации к архитектуре Grid обуславливают необходимость ориентации таких систем на технологии Web-сервисов, когда некоторый узел содержит множество сервисов, которые он предоставляет для использования другими узлами, входящими в Grid-систему. Данный подход подразумевает, что узел, содержащий сервисы, должен иметь возможность опубликовать свои требования к безопасности предоставления сервисов, а другие узлы могут эти требования прочитать. Эти функции возлагаются на средства публикации и обмена политиками. Нарушение правил политик безопасности в Grid-системе должны отображаться в векторе репутации узла в блоке, ответственном за установление доверительных отношений.

Grid является гетерогенной системой, в которой объединено множество узлов и подсетей (домены). Каждый из таких доменов имеет свои механизмы безопасности. Таким образом, требуется применение средств трансляции сущностей и мандатов, которые выполняют преобразование между различными форматами представления информационных структур (например, преобразование мандатов PKI в мандаты Kerberos), а также средств привязки пользователей, которые выполняют сопоставление прав пользователям из различных доменов.

Средства идентификации и аутентификации являются одними из наиболее важных. Субъект может с Grid-системой только в том случае, если он себя идентифицирует. Результатом идентификации является присвоение пользователю некоторых атрибутов, прав, которые позволяют в дальнейшем контролировать доступ к ресурсам. Любые отказы со стороны средств аутентификации могут служить предлогом для недоверия удаленному узлу, поэтому такие события должны четко отслеживаться и отображаться в векторе репутации блока установления доверия.

Для предлагаемых средств формирования доверия на основе репутации весьма важными являются данные от средств антивирусной защиты и обнаружения атак, поскольку угрозы, с которыми они сталкиваются, оказывают наибольшее влияние на формирование репутации узла.

Для реализации предложенного ранее метода установления доверия узлам в Grid-системе предлагается следующая структура средств обеспечения безопасности и включения в нее служб формирования и контроля уровня доверия к узлу (рис. 3). Данная структура поддерживает основные рекомендации OGF по построению системы безопасности Grid: наличие службы сетевой безопасности, службы авторизации и аутентификации, а также службы безопасности передачи сообщений, а также предполагается возможность включения и других дополнительных служб. Набор средств безопасности представляет собой четко структурированную систему, в которой каждое средство максимально независимо от другого.

Единственной службой в этой структуре, которая работает в тесном взаимодействии с другими, является служба аудита. Это одна из важнейших служб: она ведет обмен данными со службой расчета уровня доверия и формирования показателей репутации узла. Служба аудита отслеживает все события, происходящие в системе: ошибки идентификации и аутентификации, попытки атак и результаты работы антивирусных средств.

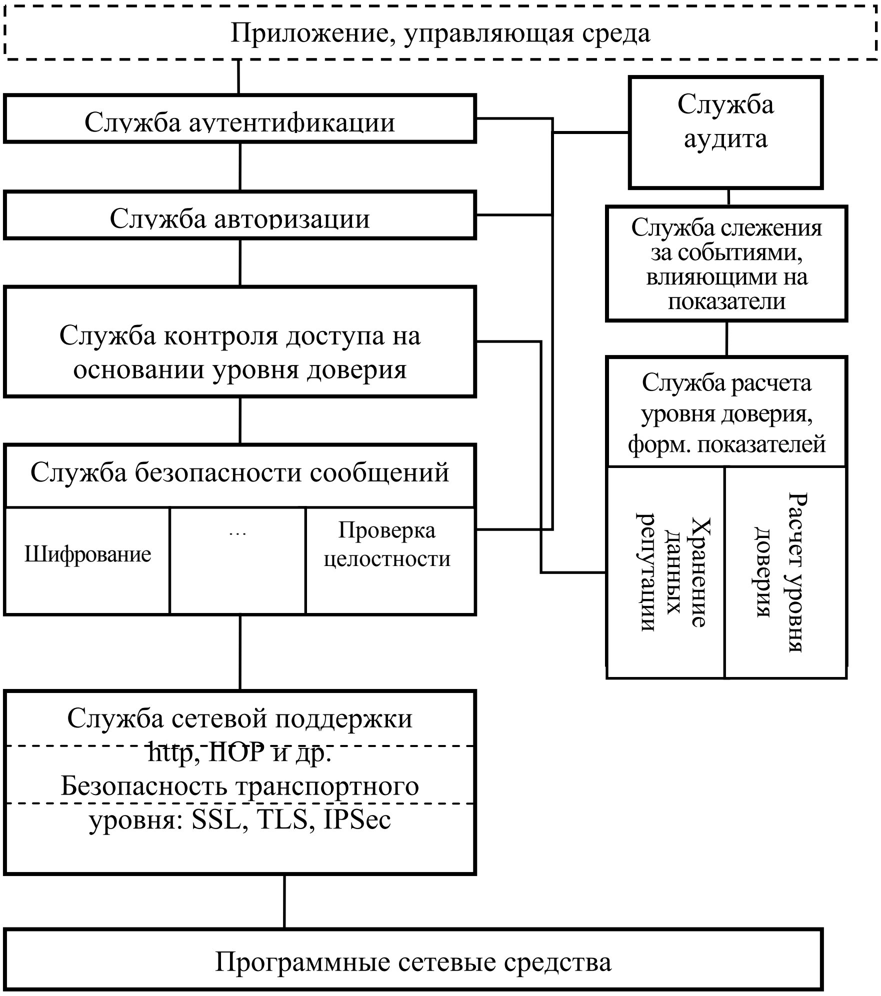


Рисунок 3 – Структура средств защиты Grid-систем, основанных на репутационном методе установления доверия

Также слежение за событиями, возникающими в системе безопасности, можно также организовать непосредственно, т.е. добавить отдельный модуль службы мониторинга, который будет обрабатывать все события, связанные с критичными действиями субъектов в системе.

Анализ уровня защищенности Grid-систем со средствами защиты на основе существующих и репутационного методов установления доверия

При проектировании комплекса средств защиты Grid-систем требуется выполнять анализ параметров разрабатываемых средств для оценки эффективности их применения.

В качестве основных параметров для оценки проектируемых средств защиты Grid выступают:

1) уровень защищенности Grid-системы;
2) ресурсозатратность на реализацию средств защиты;
3) время установления доверия к узлу;
4) вероятность корректного установления доверия.

Уровень защищенность, предоставляемый средствами защиты Grid, является одним из важнейших показателей эффективности функционирования Grid, наряду с такими показателями как надежность, отказоустойчивость, производительность и т. п.

Уровень защищенности Grid – это степень адекватности реализованных в ней механизмов защиты информации существующим для данной системы рискам безопасности, связанным с реализацией угроз безопасности информации.

В настоящее время не существует каких-либо стандартизированных методик анализа защищенности Grid и комьютерных систем в целом. Однако возможно предложить типовую методику анализа защищенности Grid-систем.

Типовая методика анализа уровня защищенности Grid-систем включает следующие шаги:

– Изучение исходных данных по особенностям функционирования Grid;
– Оценка рисков, связанных с осуществлением угроз безопасности в отношении ресурсов Grid;
– Анализ механизмов безопасности организационного уровня, политики безопасности организации и документации по обеспечению режима информационной безопасности и оценка их соответствия требованиям существующих нормативных документов, а также их адекватности существующим рискам;
– Анализ конфигурационных файлов маршрутизаторов, межсетевых экранов и прокси-серверов, осуществляющих управление межсетевыми взаимодействиями, почтовых и DNS-серверов, а также других критических элементов сетевой инфраструктуры;
– Сканирование внешних сетевых адресов в Grid;
– Сканирование ресурсов Grid;
– Анализ конфигурации серверов и рабочих станций доменов Grid с помощью специализированных программных средств.

Перечисленные методы исследования предполагают использование как активного, так и пассивного тестирования системы защиты. Активное тестирование системы защиты заключается в эмуляции действий потенциального злоумышленника по преодолению механизмов защиты. Пассивное тестирование предполагает анализ конфигурации Grid и программного обеспечения по шаблонам с использованием списков проверки. Тестирование может производиться вручную либо с использованием специализированных программных средств.

Для упрощения анализа показателя уровня защищенности будем считать, что данный уровень определяется количеством рисков, которые система может не предотвратить. Для динамически расширяемых Grid-систем при добавлении новых узлов возрастает число рисков безопасности, т.к. новые подключаемые узлы в общем случае являются ненадежными. Увеличение числа рисков вызывает снижение уровня защищенности Grid, поскольку возможна ситуация, когда вновь подключенный ненадежный узел получит конфиденциальные данные и несанкционированно воспользуется ими.

Стабильно высокий уровень защищенности характерен для таких Grid-систем, которые состоят только из одного сегмента (и не выходят за его пределы), узлы в котором проверены (принадлежат к одной организации) и между ними и Grid-системой существует достаточно высокий уровень доверия.

Расширение Grid-системы за пределы доверенного сегмента приводит к увеличению количества рисков и, как следствие, к снижению уровня защищенности. Уровень защищенности Grid экспоненциально падает с ростом числа вновь подключаемых узлов, которые характеризуются низким (или даже нулевым) уровнем доверия к ним.

Экспериментальные исследования уровня защищенности, обеспечиваемого средствами защиты Grid-систем

Для оценки уровня защищенности, предоставляемого предлагаемыми средствами обеспечения безопасности Grid-систем на основе дифференциального уровня доверия между узлами и ранжирования информации по ее ценности, проведены экспериментальные исследования.

Исследования проводились с помощью специального программного комплекса, которые имитирует взаимодействие узлов в Grid-системе и установление доверия между ними на основе предложенного репутационного метода установления доверия. При проведении экспериментов предполагалось наличие двух типов узлов: штатные узлы Grid-системы и узлы-злоумышленники (заведомо нацеленные на причинение вреда или хищения информации либо взломанные злоумышленниками узлы), при этом считается, что узлы-злоумышленники невозможно выявить на этапе их подключения к Grid-системе. В отличие от штатных узлов, узлы-злоумышленники, кроме выполнения работы, назначенной им Grid-системой, выполняют несанкционированные действия: сканирование портов, попытки доступа к защищенным ресурсам, искажение результатов вычислений, попытки передачи вирусов и т.п.

При выполнении экспериментальных исследований анализировалось то, как изменяется уровень защищенности системы при подключении к ней новых узлов путем оценки уровня опасности обработки данных в Grid. Уровень опасности определяется как отношение количества пропущенных (незаблокированных) транзакций, инициированных узлами-злоумышленниками, в ходе которых происходили неправомерные действия, к общему количеству транзакций от всех узлов, при этом уровень защищенности является обратной величиной к уровню опасности обработки данных. Значения уровня защищенности находятся в интервале от 0 (защита отсутствует) до 1 (абсолютная защита – теоретически возможный случай).

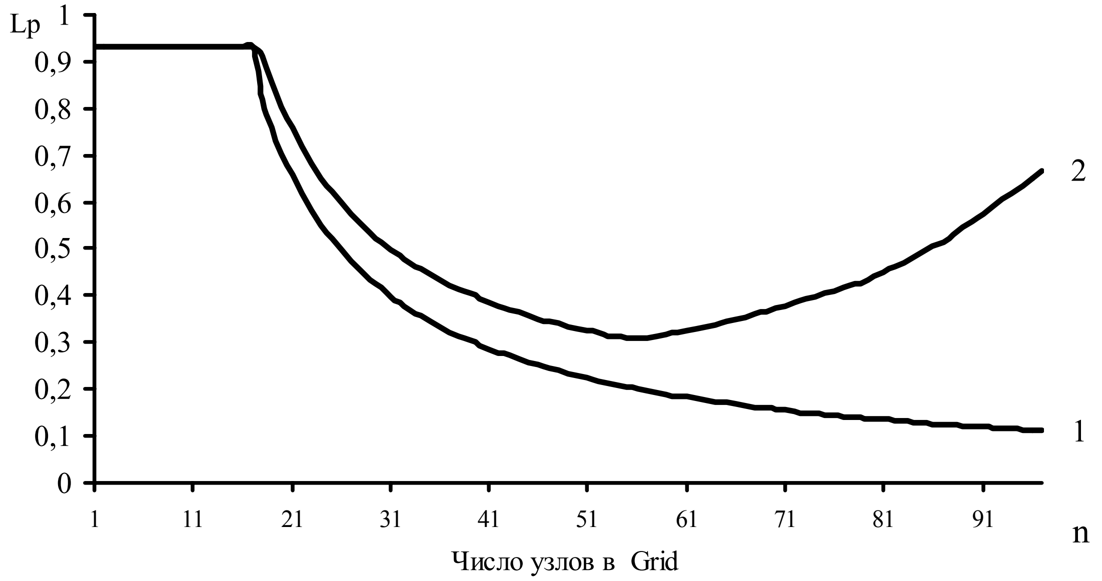


Рисунок 4 – Зависимость уровня защищенности *Lp* Grid-системы от числа добавляемых узлов *n* за некоторый период времени для средств безопасности на основе предложенной репутационного метода установления доверия узлам
1 – существующие средства защиты Grid,
2 – предложенные средства защиты Grid на основе репутационного метода

Приведенные на рис. 4 зависимости иллюстрируют преимущество предложенных средств по сравнению с традиционными подходами к организации защиты Grid-систем. Применение репутационного метода установления доверия узлам позволяет повысить уровень защищенности системы при динамическом наращивании количества узлов по сравнению с уровнем защищенности, предоставляемым существующими средствами защиты.

Снижение уровня защищенности на первом этапе вызвано временными затратами на формирование вектора репутации узлов и установления уровня доверия к ним. Повышение уровня защищенности на втором этапе вызвано тем, что число узлов с ненулевым уровнем доверия превышает число узлов с нулевым уровнем доверия.

Заключение

Средства обеспечения безопасности являются одним из важнейших элементов гарантирования штатного функционирования современных Grid-систем. Предложенные средства защиты на основе репутационного метода установления доверия между узлами и ранжирования информации по ее ценности позволяют повысить эффективность систем безопасности Grid. При применении данных средств обеспечиваемый уровень защищенности остается достаточно высоким даже при масштабировании Grid-системы с добавлением новых узлов, что особенно важно в практических приложениях.

Литература

1. The Security Architecture for Open Grid Services / Nagaratnam N., Janson P., Dayka J., Nadalin A., Siebenlist F., Welch V., Foster I., Tuecke S. – IBM Corporation, 2003. – 74 p.
2. Foster I., Kesselman C., Nick J., Tuecke S. The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration. – Springer Verlag, 2002. – 31 p.
3. Chakrabarti A. Grid Computing Security // International Workshop "Advanced Computing and Communications (ADCOM)". – Ahmedabad (INDIA). – December, 2004. – 12 p.
4. Security for Grid Services / Welch V., Siebenlist F., Foster I., Bresnahan J., Czajkowski K., Gawor J., Kesselman C., Meder S., Pearlman L., Tuecke S. // 12-th International Symposium on High Performance Distributed Computing (HPDC-12). – IEEE Press. – 2003.
5. Астахов А. Анализ защищенности корпоративных автоматизированных систем // Информационный бюллетень "Jet Info". – 2002. – 7 с.
6. Широчин В.П., Мухин В.Е., Крамар Д.И. Анализ рисков в задачах мониторинга безопасности компьютерных систем и сетей // Захист інформації. – 2003. – № 1. – С. 28-34.
7. Teo Y.M., Wang X.B. ALiCE: A Scalable Runtime Infrastructure for High Performance Grid Computing. // Proceedings of IFIP International Conference on Network and Parallel Computing, Springer Verlag. – Wuhan (China). – October 18 – 20, 2004. – P. 101-109.

В.Е. Мухін

Засоби захисту GRID-систем на основі диференціювання рівня довіри до вузлів системи

У статті запропоновано засоби захисту Grid-систем на основі репутаційного методу встановлення довірчих відносин між вузлами та ранжування інформації за її цінністю. Проведені експериментальні дослідження показали, що запропоновані засоби дозволяють підвищити рівень захищеності Grid-системи під час її масштабування з додаванням нових вузлів, що підвищує ефективність системи забезпечення безпеки Grid.

V.E. Muhin

Mechanisms for GRID Security Based on Varying of Truth-Full Level to Nodes

In this paper are suggested the mechanisms for Grid security, which are based on the reputation methods for truth-full relations between nodes and on the ranging of information by its value. The performed experimental researches have shown, that the suggested mechanisms allow to increase the security level even in case of Grid scaling with new nodes integration, that increases the efficiency of Grid safety system.

Статья поступила в редакцию 18.07.2008.